Hw

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/888,316	06/22/2001	Thomas R. Volpert JR.	22275.0002	9555

56365 7590 03/17/2006

MANISHA CHAKRABARTI
3108 S. RT. 59
STE. 124-282
NAPERVILLE, IL 60564

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/888,316	VOLPERT, THOMAS R.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,5-10,21-23 and 25-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-10,21-23 and 25-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 August 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 12/27/2005.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 1, 3, 5-10, 21-23, and 25-61 have been considered but are moot in view of the new ground(s) of rejection.

The examiner notes that in the interview held 12/15/2005, the examiner reminded the attorney to ensure that no new matter was entered and that any amendments made to the claims were fully supported by the specification. The examiner reiterated that new matter would not be allowed in the claims. As shown below, as indicate below, the specification did not provide proper support for all the newly added claim language and thus the claims have been rejected under 35 USC 112 1st Paragraph.

Claims 1, 3, 5-10, 21-23, and 25-61 have been examined. Claims 2, 4, 11-20, and 24 have been cancelled.

Regarding the previously presented rejection under 35 USC 101, the rejection has been withdrawn because, as the applicant pointed out, the result is useful (hides data), tangible (the encrypted data has a particular meaning), and concrete (reproducible).

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claims 1, 21, and 23 recite the limitations "providing a static control code index", an "index that is defined prior to receiving the input data string", and the "control codes are independent of input data string specific characteristics".

See the rejection of these claims under 35 USC 112 1st Paragraph, for further explanation.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 3, 5-10, 21-23, and 25-61 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 1, 21, and 23, the limitations "providing a static control code index", an "index that is defined prior to receiving the input data string", and the "control codes are independent of input data string specific characteristics" are not supported by the specification. Although there was disclosure of providing a control code index, there was no description of the index being static, when the index was defined, or that the index was independent of the input data string. As such, it is unclear whether applicant had possession of the invention in which the order was generated via a random number generator. Therefore, claims 1, 3, 5-10, 21-23, and 25-61 are rejected for failing to meet the written description requirement of 35 USC 112 1st Paragraph.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5, 8-10, 21-23, 25-26, 29-40, 44-55, and 29-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Maine et al. (US Patent Number 3,656,178) hereinafter referred to as De Maine, and further in view of Cellier et al. (US Patent Number 5,884,269) hereinafter referred to as Cellier.

Regarding claim 1, De Maine disclosed a method for encrypting an input data string comprising a plurality of bits of binary data using a device including a processor communicatively coupled to a memory loaded with an encryption program, the method comprising: receiving an input data string for encryption at a processor (See De Maine Col. 91 Lines 67-73); determining an order in which to query the presence of each of 2^n different configurations of n bits within an input data string (See De Maine Col. 91 Lines 67-74, 256 Byte Table); generating a code associated with the determined order (See De Maine Col. 92 Lines 5-10, Type 2 codes); generating a position code by identifying the positions of each of the 2^n different configurations of n bits in an input data string in accordance with the determined order (See De Maine Col. 92 Lines 31-39, Bit Map); and combining the control code and the position code to form an encrypted data string (See De Maine Col. 92 Lines 40-44), however, De Maine did not specifically disclose providing a static control code index that is defined prior to

receiving the input data string for encryption at the processor, the control code index including a plurality of control codes wherein the values of the plurality of control codes are independent of input data string specific characteristics, or generating a control code using the control code index.

Cellier teaches that in a coding method, a table dictionary (control code index) including a plurality of tables should be incorporated and table select (control code), for identifying which table was used in the coding method, should be included with the encoded data (See Cellier Col. 4 Line 46 – Col. 5 Line 55 and Col. 13 Lines 24-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Cellier in the coding system of De Maine by providing a table dictionary including tables (See De Maine Col. 91 Lines 67-74) which are identified using a table select (control code) and including the table select with the encoded data in order to allow the decoder to identify which table was used for encoding. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a highly efficient and compact way of mapping the statistics of the input string in order to identify the optimum encoding table.

Regarding claim 21, De Maine disclosed a method for encrypting an input data string comprising a plurality of bits of binary data (See De Maine Col. 2 Paragraph 1), the method comprising: using a software program code means embodied on a computer readable medium, receiving an input data string for encryption (See De Maine Col. 91 Lines 67-74); using a software program code means embodied on a computer readable medium, determining an order

in which to query the presence of each of 2^n different configurations of n bits within an input data string (See De Maine Col. 91 Lines 67-74, 256 Byte Table); using a software program code means embodied on a computer readable medium, generating a code associated with the determined order (See De Maine Col. 92 Lines 5-10, Type 2 codes); using a software program code means embodied on a computer readable medium, generating a position code by identifying the positions of each of the 2^n different configurations of n bits in an input data string in accordance with the determined order (See De Maine Col. 92 Lines 31-39, Bit Map); and using a software program code means embodied on a computer readable medium, combining the control code and the position code to form an encrypted data string (See De Maine Col. 92 Lines 40-44), however, De Maine did not specifically disclose providing a static control code index that is defined prior to receiving the input data string for encryption at the processor, the control code index including a plurality of control codes wherein the values of the plurality of control codes are independent of input data string specific characteristics, or generating a control code using the control code index.

Cellier teaches that in a coding method, a table dictionary (control code index) including a plurality of tables should be incorporated and table select (control code), for identifying which table was used in the coding method, should be included with the encoded data (See Cellier Col. 4 Line 46 – Col. 5 Line 55 and Col. 13 Lines 24-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Cellier in the coding system of De Maine by providing a table dictionary including tables (See De Maine Col. 91 Lines 67-74) which are identified using

a table select (control code) and including the table select with the encoded data in order to allow the decoder to identify which table was used for encoding. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a highly efficient and compact way of mapping the statistics of the input string in order to identify the optimum encoding table.

Regarding claim 23, De Maine disclosed a computer usable medium storing a computer program for encrypting an input data string comprising a plurality of bits of binary data (See De Maine Col. 2 Paragraph 1), the method comprising: computer readable code for receiving an input data string for encryption; computer readable code for determining an order in which to query the presence of each of 2^n different configurations of n bits within an input data string (See De Maine Col. 91 Lines 67-74, 256 Byte Table); computer readable code for generating a code associated with the determined order (See De Maine Col. 92 Lines 5-10, Type 2 codes); computer readable code for generating a position code by identifying the positions of each of the 2^n different configurations of n bits in an input data string in accordance with the determined order (See De Maine Col. 92 Lines 31-39, Bit Map); and computer readable code for combining the control code and the position code to form an encrypted data string (See De Maine Col. 92 Lines 40-44), however, De Maine did not specifically disclose providing a static control code index that is defined prior to receiving the input data string for encryption at the processor, the control code index including a plurality of control codes wherein the values of the plurality of control codes are independent of input data string specific characteristics, or generating a control code using the control code index.

Cellier teaches that in a coding method, a table dictionary (control code index) including a plurality of tables should be incorporated and table select (control code), for identifying which table was used in the coding method, should be included with the encoded data (See Cellier Col. 4 Line 46 – Col. 5 Line 55 and Col. 13 Lines 24-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Cellier in the coding system of De Maine by providing a table dictionary including tables (See De Maine Col. 91 Lines 67-74) which are identified using a table select (control code) and including the table select with the encoded data in order to allow the decoder to identify which table was used for encoding. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a highly efficient and compact way of mapping the statistics of the input string in order to identify the optimum encoding table.

Regarding claims 3 and 25, De Maine and Cellier disclosed determining an order comprises selecting a predetermined order (See De Maine Col. 91, 256 Byte Table and the rejection of claim 1 above).

Regarding claims 5, 22, and 26, De Maine and Cellier disclosed dividing the input data string into a plurality of blocks of data (See De Maine Col. 92 Lines 31-38).

Regarding claim 8, and 30, De Maine and Cellier disclosed generating a plurality of block codes associated with a plurality of blocks of data, each block code indicating the number of bits within the associated block of data (See De Maine Col. 101 Lines 45-52).

Regarding claim 9, and 31, De Maine and Cellier disclosed combining the each of the plurality of block codes with the control code and the position code for the associated block of data (See De Maine Col. 101 Lines 45-52 and the rejection of claim 1 above).

Regarding claim 10, and 32, De Maine and Cellier disclosed that determining an order comprises determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string (See De Maine Col. 101 Lines 20-25).

Regarding claims 29, and 50, De Maine and Cellier disclosed that the computer readable code for determining an order further comprises computer readable code for determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order (See De Maine Col. 91 Lines 67-74).

Regarding claim 33, De Maine and Cellier disclosed that the computer readable code for determining an order further comprises computer readable code for determining an order in which to query the presence of each of 2^n different configurations of n bits based on an analysis of the input data (See De Maine Col. 91 Lines 67-74).

Regarding claims 34 and 48, De Maine and Cellier disclosed generating the control code based on the input string (See De Maine Col. 91 Lines 67-74 and the rejection of claim 1 above), but failed to disclose randomly generating the control code. However, it was well known in the art at the time of invention that an input to a function could be random. It therefore would have been obvious to the ordinary person skilled in the art at the time of invention that when the input was random, the control code generated would also be random since it was based on the input.

This would have been obvious because the ordinary person skilled in the art would have used what was well known in the art to come to this conclusion.

Regarding claims 35, and 49, De Maine and Cellier disclosed generating the control code based on a mathematical formula (See De Maine Col. 91 Lines 67-74 and the rejection of claim 1 above)

Regarding claims 36 and 51, De Maine and Cellier disclosed determining whether the input data string can be compressed simultaneously as it is encrypted (See De Maine Col. 101 Lines 20-28).

Regarding claims 37 and 52, De Maine and Cellier disclosed dividing the input data string into n bit sequences (See De Maine Col. 91 Lines 67-74); comparing each of the 2^n different configurations of n bits with each of the n bit sequences (See De Maine Col. 91 Lines 67-74); determining the frequency of each of the 2^n different configurations appearing in the input data string (See De Maine Col. 91 Lines 67-74); determining whether a specific relationship exists between values of the frequencies of each of the individual 2^n different configurations appearing in the input date string wherein the existence of the specific relationship is indicative of the presence of a characteristic within the input data string and wherein the presence of the characteristic indicates that the input data string can be compressed simultaneously as it is encrypted (See De Maine Col. 101 Lines 20-25); selecting a first position code routine associated with the determined order when the specific relationship exists, the first position code being operable to encrypt and compress the input data string (See De Maine Col.

101 Lines 20-25 and Col. 92 Paragraphs 1-2); and selecting a second position code routine associated with the determined order when the specific relationship does not exist, the second position code being operable to encrypt the input data string without any compression (See De Maine Col. 101 Lines 20-25 and Col. 92 Paragraphs 1-2).

Regarding claims 38 and 53, De Maine and Cellier disclosed that the determining the order in which to query the presence of each of 2^n different configurations of n bits within an input data string comprises computer readable code for determining the order in which to query the presence of each of 2^2 different configurations of 2 bits within an input data string (See De Maine Col. 91 Lines 47-48).

Regarding claims 39 and 54, De Maine and Cellier disclosed dividing the input data string into n bit sequences (See De Maine Col. 91 Lines 67-74); comparing each of the 2^n different configuration of n bits with each of the n bit sequences of the input data string (See De Maine Col. 91 Lines 67-74); determining a first number representative of the number of times the most frequently occurring 2^n configuration appears in the input string; determining a second number representative of the number of times the second most frequently occurring 2^n configuration appears in the input string; determining a third number representative of the number of times the third most frequently occurring 2^n configuration appears in the input string determining a fourth number representative of the number of times the fourth most frequently occurring 2^n configuration appears in the input string (See De Maine Col. 91 Lines 67-74); selecting a first position code routine associated with the determined order when the first number is greater than the sum of the third number and the fourth number, the first position code routine

being operable to encrypt and compress the input data string (See De Maine Col. 92 Paragraphs 1-2 and Col. 101 Lines 20-27); and selecting a second position code routine associated with the determined order when the first number is not greater than the sum of the third number and the fourth number, the second position code routine being operable to encrypt the input data string without any compression (See De Maine Col. 92 Paragraphs 1-2 and Col. 101 Lines 20-27).

Regarding claims 40 and 55, De Maine and Cellier disclosed that generating a control code associated with the determined order, further comprises: generating a first control code associated with the determined order when the first position code routine is selected; and generating a second control code associated with the determined order when the second position code routine is selected wherein the first control code is different than the second control code (See De Maine Col. 92 Paragraphs 1-2).

Regarding claims 44 and 59, De Maine and Cellier disclosed selecting a default order (See De Maine Col. 91 Lines 67-74 and the rejection of claim 1 above).

Regarding claims 45-46 and 60-61, De Maine and Cellier disclosed determining an order based on the relative frequencies of the combinations of n bits (See De Maine Col. 91 Lines 67-74).

Regarding claim 47, De Maine and Cellier disclosed determining the order based on an analysis of the input data string (See De Maine Col. 91 Lines 67-74).

Claims 6-7, and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Maine and Cellier as applied to claims 5, and 26 respectively, and further in view of Shimizu et al. (US Patent Number 6,772,343) hereinafter referred to as Shimizu.

De Maine and Cellier disclosed blocking the input data into block sizes of a certain range (See De Maine Col. 92 Lines 31-38) but failed to disclose determining the size of the blocks randomly or mathematically.

Shimizu teaches that in a block encoding system, generating each block size randomly makes illicit access of the data more difficult and makes the cryptosystem more robust (See Shimizu Col. 5 Lines 9-18). Shimizu further teaches that the random sizes are generated mathematically using a seed (See Shimizu Col. 15 Paragraphs 3-7).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Shimizu in the invention of De Maine and Cellier to mathematically generate random block lengths. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the added security of random block lengths to the compressed data.

Claims 41-42, and 56-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Maine and Cellier as applied to claim 1 above, and further in view of Weiss (US Patent Number 5,479,512).

De Maine and Cellier disclosed compressing input data (See De Maine Cols. 91-92), but failed to disclose re-encrypting the data after the compression was performed.

Weiss teaches that after compression is performed, the compressed data should be XORed with a key, in small blocks at a time (See Weiss Col. 5 Paragraphs 4-5 and Col. 6 Paragraph 3 and Fig. 3A).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Weiss in the compression system of De Maine and Cellier by XORing the coded data with a key in small blocks at a time. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the data from unauthorized observing.

Claims 41, 43, 56, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Maine and Cellier as applied to claim 1 above, and further in view of Butler et al. (US Patent Number 5,861,887) hereinafter referred to as Butler.

De Maine and Cellier disclosed compressing input data (See De Maine Cols. 91-92), but failed to disclose re-encrypting the data after compression was performed.

Butler teaches that compression should be repeated as many times as necessary in order to make the data being compressed sufficiently small (See Butler Col. 3 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Butler in the compression system of De Maine and Cellier by repeating the compression on the coded output as many times as necessary to get the output to be sufficiently small. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide more efficient storage of the audio data.

Conclusion

Claims 1, 3, 5-10, 21-23, and 25-61 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
3/14/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100